MATAN SHTEPEL

(925) · 922 · 9254 ◇ matan.shtepel@gmail.com ◇ matanshtepel.com

Last updated: July. 2023. ◇ Most recent version: https://matanshtepel.com/matan_shtepel_cv.pdf

OVERVIEW

I'm a junior cryptography researcher, so far mainly working on Secure Multiparty Computation (MPC) and Oblivious RAM (ORAM). I plan to apply to P.h.D. programs in cryptography in December'23. Outside broad fascination in theoretical CS and math, I am also interested in blockchains (ETH in particular), Australian rock music, math, Bob Dylan, and rationality.

EDUCATION

University of California, Los Angeles Sep. 2021 - March 2023
B.S.E Computer Science (concentration in Pure Math) with honors.
Research in cryptography
Primary advisor: Prof. Rafail Ostrovsky (UCLA)
Secondary advisor: Prof. Brett Falk (Upenn)
Organized UCLA Theoretical Computer Science Guild

Las Positas Community College June 2020 - May 2021
A.S Computer Science with honors.
A.S Math with honors.
Honors project advised by Dr. William Pezzaglia: Quaternion-based Graphics

PUBLICATIONS

Authors in alphabetical order unless stated otherwise.

- **GigaDORAM: Breaking the Billion Address Barrier**
  We construct and implement the most practically efficient Distributed Oblivious RAM (DORAM) protocol to date, outperforming all existing DORAM constructions by over 400x. We hope our construction will enable RAM-MPC to be deployed in practice.
  B. Falk, R. Ostrovsky, M. Shtepel, J. Zhang
  Accepted to USENIX '23

- Mark Burgin, Matan Shtepel. On totalisation of Computable Functions in a Distributive Environment
  International Journal of Parallel, Emergent and Distributed Systems, Volume 37, Number 3, October 2021.

In-Submission

- **DORAM revisited: Maliciously secure RAM-MPC with logarithmic overhead**
  We give the first malicious construction of Distributed ORAM while matching the asymptotics of the best-known semi-honest constructions. As a corollary, we give the *first* maliciously-secure MPC with logarithmic random access overhead.
  B. Falk, D. Noble, R. Ostrovsky, M. Shtepel, J. Zhang
  Submitted to TCC'23

Other research in progress

Currently working on projects on topics: Succinct Non-Interactive Arguments (SNARGs), weighted MPC, MPC lower bounds, and additional aspects of the practice & theory of Distributed Oblivious RAM. I hope to submit at least two of those works in Fall'23.

FUNDING & AWARDS

- **NSF REU funding for summer 2023.** Granted for work on secure multiparty computation advised Prof. Rafail Ostrovsky at UCLA.

- **NSF REU funding for summer 2022.** Granted for work on secure multiparty computation advised Prof. Rafail Ostrovsky at UCLA.
- **The 10'th Heidelberg Laureate Forum.** One of 200 young researchers (undergraduates, graduates, and postdoctoral fellows) worldwide invited to the 10'th Heidelberg Laureate Forum.
- **Outliers 23'.** Participate in competitively selected applied cryptography/web3 focused, VC-backed, summer program.
- **Hack Lodge (sponsored by ETH university) 2023.** Participate in competitively selected applied cryptography/Ethereum ecosystem-focused hacker house.

NON-RESEARCH ACADEMIC ACTIVITIES

Undergraduate Research Mentor Oct 2022 - present
Cryptography research at UCLA

- Mentor Stephen Kelman on a cryptography research project, with a focus on implementing high-performance, novel MPC protocols in `C++`. We plan to contribute open-source code enabling MPC in the RAM model to EMP Toolkit and hope to submit a corresponding publication. Under Prof. Rafail Ostrovsky's guidance.
- Mentor Nakul Khambhati on a cryptography research project with a proving lower bounds on sublinear message complexity information-theoretic MPC. Under Prof. Rafail Ostrovsky's guidance.

Founder & Organizer Sep 2022 - May 2023
UCLA Theory Guild

- Found and organize the UCLA Theoretical Computer Science Guild, UCLA's (first?) theoretical computer science community. Meet on a weekly basis, to discuss various readings in theoretical computer science. "Fuild" will continue in Fall'23 under Nakul Khambhati's leadership.

Prepare Students for P.h.D. Program May 2023 - Sep 2023
UCLA Undergraduate Research Center

- Lead a program for UCLA students interested in pursuing a STEM P.h.D.

Advocate for Community College Researchers Sep 2022 - present
UCLA Engineering Transfer Center

- Invited to speak on the Engineering Research Presentations & Panel (only transfer student) at UCLA Engineering Day.
- Invited to speak at the Engineering Transfer Day Research Panel (only current undergraduate) at UCLA Engineering Transfer Day.
- Research-oriented talk Las Positas / Chabot Community College (expected, September 2023)

WORK EXPERIENCE

AppReciate iOS App June 2023 - present
App Development

- Design and build (together with Victoria Nguyen) an app to help people appreciate the often-trivialized beauties of life

STEM Tutor July 2019 - March 2021
Matan's Tutoring Business & Pleasanton Unified School District *Pleasanton, CA*

- Independently tutor middle and high school students primarily in math, but also in biology, programming, and history.
  - Over the entire period, had about 7 students, on average meeting with 3 students a week, each for an hour.
- Tutored for the Pleasanton Unified School District

- Tutor at Fairlands Elementary School after-school program, twice a week during the 2019 schoolyear until COCIV (march 2019).
- Tutor at summer school 2019 for English and math.

Founder, Designer, Advertiser, ... June 2019 - June 2020
RAWGNARLY! (fashion brand) *Pleasanton, CA*

- Founded and operated RAWGNARLY! a fashion brand all about having not-too-serious fun with your friends.
- Sold about 120 garments, both locally in Pleasanton (about 100) and all across the US (about 20).
- Designed garments, photographed lookbooks, created advertisements, built website, negotiated with vendors (US & abroad).

Sales Associate, Pizzaboy August 2018 - May 2019
Skechers & Pizza Guys *Livermore, Pleasanton, CA*

- Retail associate at Skechers Footwear at the Livermore outlets and cook at Pizza Guys' Pleasanton branch.

RELEVANT COURSEWORK

Graduate cryptography sequence + special topics (winter 23'), graduate communication complexity theory, graduate quantum computing, graduate computational complexity theory (winter 23'), graduate theory hits of 21'st century (winter 23'), real analysis sequence, probability theory sequence, linear algebra sequence, group theory, enumerative combinatorics, required CS curriculum.